

ON KLOOSTERMAN SUMS OVER FINITE FIELDS OF CHARACTERISTIC 3

L. A. BASSALYGO AND V.A. ZINOVIEV

ABSTRACT. We study the divisibility by 3^k of Kloosterman sums $K(a)$ over finite fields of characteristic 3. We give a new recurrent algorithm for finding the largest k , such that 3^k divides the Kloosterman sum $K(a)$. This gives a new simple test for zeros of such Kloosterman sums.

1. INTRODUCTION

Let $\mathbb{F} = \mathbb{F}_q$ be a field of characteristic p of order $q = p^m$, where $m \geq 2$ is an integer and let $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. By \mathbb{F}_p denote the field, consisting of p elements. For any element $a \in \mathbb{F}^*$ the *Kloosterman sum* can be defined as

$$(1.1) \quad K(a) = \sum_{x \in \mathbb{F}} \omega^{\text{Tr}(x+a/x)},$$

where $\omega = \exp 2\pi i/p$ is a primitive p -th root of unity and

$$(1.2) \quad \text{Tr}(x) = x + x^p + x^{p^2} + \dots + x^{p^{m-1}}.$$

Recall that under x^{-i} we understand x^{p^m-1-i} , avoiding by this way a division into 0.

Kloosterman sums are used for solutions of equations over finite fields [19], in the theory of error correcting codes [18], for studying and constructing of bent and hyperbent functions [8, 16] and so on. Surely, any Kloosterman sum $K(a)$ for a given a can be found directly computing its value for every element of the field, but this method requires a large amount of computations, which is a multiple of the size of the field. Hence more simple methods of computations of Kloosterman sums are quite interesting. The values of characteristic $p \in \{2, 3\}$ are especially interesting in connection with the number of q -rational points of some elliptic curves [17, 18, 20, 23]. Divisibility of binary Kloosterman sums by numbers 8, 16, \dots , 256 and computations of such sums modulo some numbers was considered in papers [6, 7, 14, 10, 11, 12, 15, 20, 21, 24]. Divisibility of ternary Kloosterman sums $K(a)$ by 9 and by 27 was considered in [11, 12, 13, 14, 20, 21].

2010 *Mathematics Subject Classification.* Primary 11T23; Secondary 11L05.

Key words and phrases. Kloosterman sums over \mathbb{F}_{3^m} , divisibility by 3^k , zeros of Kloosterman sums.

THIS WORK HAS BEEN PARTIALLY SUPPORTED BY THE RUSSIAN FUND OF FUNDAMENTAL RESEARCHES (NUMBER OF PROJECT 15 - 01 - 08051).

Furthermore, in [11, 12, 13] a complete characterization of $K(a)$ modulo 9, 18 and 27 was obtained for any m and a .

In the recent papers [2, 3] we provide two algorithms to find the maximum divisor of $K(a)$ of type 2^k . Similar results for the case $p = 3$ have been announced in [4] and here we prove these results. In particular, we give a simple test of divisibility of $K(a)$ by 27. We suggest also a new recursive algorithm of finding the largest divisor of $K(a)$ of the type 3^k which needs at every step the limited number of arithmetic operations in \mathbb{F} . For the case when $m = gh$ we derive the exact connection between the divisibility by 3^k of $K(a)$ in \mathbb{F}_{3^g} , $a \in \mathbb{F}_{3^g}$, and the divisibility by $3^{k'}$ of $K(a)$ in $\mathbb{F}_{3^{gh}}$.

2. KNOWN RESULTS

In this section we state the known results about Kloosterman sums $K(a)$ [20, 23] and elliptic curves $E(a)$ [9, 22] over finite fields \mathbb{F} of characteristic 3. Our interest is the divisibility of such sums by the maximal possible number of type 3^k (i.e. 3^k divides $K(a)$, but 3^{k+1} does not divide $K(a)$; in addition, when $K(a) = 0$ we assume that 3^m divides $K(a)$, but 3^{m+1} does not divide; recall that $q = 3^m = |\mathbb{F}|$).

For a given \mathbb{F} and any $a \in \mathbb{F}^*$ define the elliptic curve $E(a)$ as follows:

$$(2.1) \quad E(a) = \{(x, y) \in \mathbb{F} \times \mathbb{F} : y^2 = x^3 + x^2 - a\}.$$

The set of \mathbb{F} -rational points of the curve $E(a)$ over \mathbb{F} forms a finite abelian group, which can be represented as a direct product of a cyclic subgroup $G(a)$ of order 3^t and a certain subgroup $H(a)$ of some order s (which is not multiple to 3): $E(a) = G(a) \times H(a)$, such that

$$|E(a)| = 3^t \cdot s$$

for some integers $t \geq 2$ and $s \geq 1$ (see [9]), where $s \not\equiv 0 \pmod{3}$.

Moisio [23] showed that

$$(2.2) \quad |E(a)| = 3^m + K(a),$$

where $|A|$ denotes the cardinality of a finite set A (earlier the same result was obtained in [17] for the curve $y^2 + xy + ay = x^3$). Therefore a Kloosterman sum $K(a)$ is divisible by 3^t , if and only if the number of points of the curve $E(a)$ is divisible by 3^t . Lisonek [20] observed, that $|E(a)|$ is divisible by 3^t , if and only if the group $E(a)$ contains an element of order 3^t .

Since $|E(a)|$ is divisible by $|G(a)|$, which is equal to 3^t , then generator elements of $G(a)$ and only these elements are of order 3^t .

Let $Q = (\xi, *) \in E(a)$. Then the point $P = (x, *) \in E(a)$, such that $Q = 3P$ exists, if and only if the equation

$$x^9 - \xi x^6 + a(1 - \xi)x^3 - a^2(a + \xi) = 0.$$

has a solution in \mathbb{F} (see [9]). This equation is equivalent to equation

$$(2.3) \quad x^3 - \xi^{1/3}x^2 + (a(1 - \xi))^{1/3}x - (a^2(a + \xi))^{1/3} = 0.$$

The equation (2.3) is solvable in \mathbb{F} if and only if (see, for example, [1])

$$(2.4) \quad \text{Tr} \left(\frac{a\sqrt{\xi^3 + \xi^2 - a}}{\xi^3} \right) = 0.$$

Since the point $(a^{1/3}, a^{1/3})$ of $E(a)$ has the order 3, and hence belongs to $G(a)$, then solving the recursive equation

$$(2.5) \quad x_i^3 - x_{i-1}^{1/3}x_i^2 + (a(1 - x_{i-1}))^{1/3}x_i - (a^2(a + x_{i-1}))^{1/3} = 0, \quad i = 0, 1, \dots$$

with initial value $x_0 = a^{1/3}$, we obtain that the point $(x_i, *) \in G(a)$ for $i = 0, 1, \dots, t-1$, and the point $(x_{t-1}, *)$ is a generator element of $G(a)$. Such algorithm of finding of cardinality of $G(a)$ was given in [1].

Similar method was presented in our previous papers [2, 3] for finite fields of characteristic 2. Besides, some another results have been obtained in [2, 3] for the case $p = 2$. Our purpose here is to generalize these results for finite fields of characteristic 3.

3. NEW RESULTS

We begin with a simple result. It is known [1, 14, 21], that 9 divides $K(a)$ if and only if $\text{Tr}(a) = 0$. In this case a can be presented as follows: $a = z^{27} - z^9$, where $z \in \mathbb{F}$, and, hence $x_0 = a^{1/3} = z^9 - z^3$ (see (2.5)). We found the expression for the next element x_1 , namely:

$$x_1 = (z^4 - 1)(z^3 - 1)z^2$$

and, therefore, from the condition (2.4), the following result holds.

Proposition 3.1. *Let $a \in \mathbb{F}^*$ and $\text{Tr}(a) = 0$, i.e. a can be presented in the form: $a = z^{27} - z^9$. Then $x_0 = z^9 - z^3$, $x_1 = (z^4 - 1)(z^3 - 1)z^2$, and, therefore, $K(a)$ is divisible by 27, if and only if*

$$(3.1) \quad \text{Tr} \left(\frac{z^5(z - 1)(z + 1)^7}{(z^2 + 1)^3} \right) = 0,$$

This condition (3.1) is more compact than the corresponding condition from the papers [12, 13], where it is proven that $K(a)$ is divisible by 27, if $\text{Tr}(a) = 0$ and

$$2 \sum_{1 \leq i \leq j \leq m-1} a^{3^i+3^j} + \sum_{1 \leq i < j < k \leq m-1} a^{3^i+3^j+3^k} = 0.$$

Emphasize once more, that similar conditions permit in [11, 12, 13] to find all values of $K(a)$ modulo 9, 18 and 27, while the condition (3.1) gives only divisibility of $K(a)$ by 27.

Similar to the case $p = 2$ [2, 3], we give now also another algorithm to find the maximal divisor of $K(a)$ of the type 3^t , which requires at every step the limited number of arithmetic operations in \mathbb{F} .

Let $a \in \mathbb{F}^*$ be an arbitrary element and let u_1, u_2, \dots, u_ℓ be a sequence of elements of \mathbb{F} , constructed according to the following recurrent relation (compare with (2.5)):

$$(3.2) \quad u_{i+1} = \frac{(u_i^3 - a)^3 + au_i^3}{(u_i^3 - a)^2}, \quad i = 1, 2, \dots,$$

where $(u_1, *) \in E(a)$ and

$$(3.3) \quad \text{Tr} \left(\frac{a\sqrt{u_1^3 + u_1^2 - a}}{u_1^3} \right) \neq 0.$$

Then the following result is valid.

Theorem 3.2. *Let $a \in \mathbb{F}^*$ and let u_1, u_2, \dots, u_ℓ be a sequence of elements of \mathbb{F} , which satisfies the recurrent relation (3.2), where the element u_1 satisfies (3.3) and $(u_1, *) \in E(a)$. Then there exists an integer $k \leq m$ such that one of the two following cases takes place:*

- (i) *either $u_k = a^{1/3}$, but the all previous elements u_i are not equal to $a^{1/3}$;*
 - (ii) *or $u_{k+1} = u_{k+1+r}$ for a certain r and the all elements u_i are different for $i < k+1+r$.*
- In the both cases the Kloosterman sum $K(a)$ is divisible by 3^k and is not divisible by 3^{k+1} .*

Proof. Let $a \in \mathbb{F}^*$ and let u_1, u_2, \dots, u_ℓ be a sequence of elements of \mathbb{F} , which satisfies the recurrent relation (3.2), where the element u_1 satisfies (3.3) and the point $P_1 = (u_1, *)$ belongs to $E(a)$. Assume that $E(a)$ has the order $3^t \cdot s$, where s is prime to 3. We have to show that $k = t$.

Denote $P_i = (u_i, *)$. Since $P_1 = (u_1, *)$ belongs to $E(a)$, it follows from the addition operation in the additive abelian group $E(a)$ (Table 2.3 in [9]) and from (3.2), that for $i \geq 2$ all points P_i belongs to $E(a)$ and $P_i = 3^{i-1}P_1$ for $i \geq 2$.

There are only two possibilities: either $P_1 \in G(a)$, or $P_1 \in E(a) \setminus G(a)$.

First consider the case $P_1 \in G(a)$. We claim that the condition (3.3) implies that P_1 is a generating element of the (cyclic) group $G(a)$. Indeed, assume that it is not the case. Then it means that there is the point $Q \in G(a)$ such that $P_1 = 3Q$. Assuming that $Q = (x, *)$ and using the addition operation in $E(a)$ [9], we arrive to the following equation for x :

$$x^3 - u_1^{1/3}x^2 + (a(1 - u_1))^{1/3}x - (a^2(a + u_1))^{1/3} = 0.$$

As we already mentioned in Section 2, this equation has a solution, if and only if

$$\mathrm{Tr} \left(\frac{a\sqrt{u_1^3 + u_1^2 - a}}{u_1^3} \right) = 0,$$

that contradicts to (3.3). We conclude that P_1 is a generating point of $G(a)$ and, therefore, has the order 3^t . This means that the point $P_t = (u_t, *) = 3^{t-1}P_1$ is of the order 3. Since there are exactly two points in $E(a)$ of the order 3 [9], namely, the points $(a^{1/3}, \pm a^{1/3})$, it means that for any $i \leq t-1$ we have that $u_i \neq a^{1/3}$. Therefore, $k = t$ and $K(a)$ is divisible by 3^t .

Now consider the case when $P_1 \in E(a) \setminus G(a)$. Then the order d of the point $3^t P_1 = (u_{t+1}, *)$ divides s . The point $d P_1$ belongs to the cyclic group $G(a)$, and it is a generating element, since the equality $d P_1 = 3Q$ for some $Q \in E(a)$ implies the equality $P_1 = 3Q'$, that contradicts to (3.3). Therefore the order of the point P_1 is equal to $d \cdot 3^t$ and $K(a)$ is divisible by 3^t .

Denote by r the least integer, such that d divides $3^r - 1$ or $3^r + 1$. Then we have the following equalities:

in the first case

$$3^{t+r} \cdot P_1 = 3^t \cdot P_1$$

and in the second case

$$3^{t+r} \cdot P_1 = -3^t \cdot P_1.$$

In the both cases we obtain, that $u_{t+1} = u_{t+1+r}$ and our sequence u_1, u_2, \dots, u_ℓ becomes periodic with a period r , starting from the element u_{t+1} . \square

Remark 3.3. It is clear, that, for the case (ii) of Theorem 1, this algorithm needs $k+r$ computations of values

$$x^3 - a + \frac{a x^3}{(x^3 - a)^2}$$

for finding the largest divisor of $K(a)$ of the type 3^k . Besides, the following lower bound for the number of \mathbb{F} -rational points of the curve $E(a)$ is valid:

$$|E(a)| \geq 3^k(2r+1)$$

and, respectively, the following upper bound for the value of Kloosterman sum $K(a)$ takes place:

$$K(a) \leq 3^m - 3^k(2r+1).$$

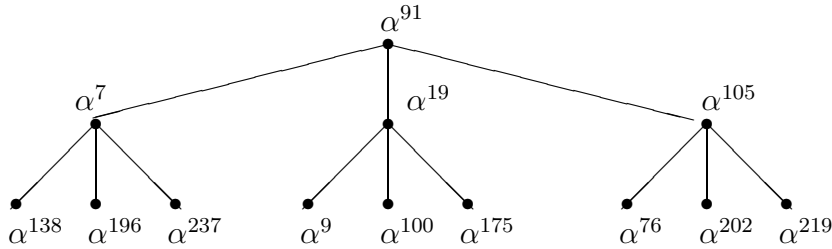
Directly from Theorem 3.2 we obtain the following necessary and sufficient condition for an element $a \in \mathbb{F}^*$ to be a zero of the Kloosterman sum $K(a)$.

Corollary 3.4. *Let $a \in \mathbb{F}^*$ and u_1, u_2, \dots, u_ℓ be a sequence of elements of \mathbb{F} of the order $|\mathbb{F}| = 3^m$, which satisfies the recurrent relation (3.2), where the element u_1 satisfies (3.3). Then $K(a) = 0$, if and only if $u_m = a^{1/3}$, and $u_i \neq a^{1/3}$ for all $1 \leq i \leq m - 1$.*

Example 3.5. Suppose the field \mathbb{F} of order 3^5 is generated by $\phi(x) = x^5 + x^4 + x^2 + 1$ and its root α is a primitive element of \mathbb{F} . Take $a = \alpha^{31}$. Following to Statement 3.7, present a as $a = z^{27} - z^9$. We find that $z \in \{\alpha^{16}, \alpha^{106}, \alpha^{231}\}$. The corresponding possible values of x_1 are α^7, α^{19} and α^{105} , respectively. For all these values of z the condition (3.1) is satisfied. We conclude that $K(a)$ is divisible by 27. Choosing $x_1 = \alpha^7$ and solving the cubic equation (2.5), we obtain three solutions for x_2 , namely, $x_2 \in \{\alpha^{138}, \alpha^{196}, \alpha^{237}\}$. Choose $x_2 = \alpha^{138}$. Then the condition (2.4) (with $\xi = x_2$) is not valid:

$$\text{Tr} \left(\frac{a \sqrt{x_2^3 + x_2^2 - a}}{x_2^3} \right) = \text{Tr}(\alpha^{202}) = 1.$$

It means that we find the exact divisor 3^k of $K(\alpha^{31})$ and the maximal cyclic subgroup $G(\alpha^{31})$ of the curve $E(\alpha^{31})$ is of the order 27. The x -th coordinates of all points $(x, *)$ of the cyclic group $G(\alpha^{31})$ are presented below as a graph, which gives all possible nine sequences $x_0 = a^{1/3}, x_1, x_2$.



As the condition (2.4) for all elements of the last third level (numeration of the levels $0, 1, \dots$ is starting from the top) is not satisfied, then $k = 3$, and we conclude that $K(\alpha^{31})$ is divisible by 27 (indeed, $K(\alpha^{31}) = 27$). Note that all points $P_i = (x_i, y_i)$, corresponding to the i -th level of the graph satisfy the condition $3^{i+1}P_i = \mathcal{O}$, where \mathcal{O} is the identity element of the group $E(a)$.

Now start from the down, choosing the point $u_1 = \alpha^{159}$, which satisfies (3.3). Then using (3.2), we obtain the sequence

$$\alpha^{159}, \alpha^{15}, \alpha^{44}, \alpha^{162}, \alpha^{162}, \dots$$

We conclude that $k = 3$ (see Theorem 3.2) and $K(a)$ is divisible by 3^3 (here $r = 1$). The choice $u_1 = \alpha^{193}$ results in the following sequence:

$$\alpha^{193}, \alpha^{199}, \alpha^{50}, \alpha^{197}, \alpha^{223}, \alpha^{197} \alpha^{223}, \dots$$

We again conclude that $k = 3$ (and here $r = 2$).

Assume now that the field \mathbb{F}_q of order $q = 3^m$ is embedded into the field \mathbb{F}_{q^n} ($n \geq 2$), and a is an element of \mathbb{F}_q^* . Recall that

$$\mathrm{Tr}_{q^n \rightarrow q}(x) = x + x^q + x^{q^2} + \dots + x^{q^{n-1}}, \quad x \in \mathbb{F}_{q^n}.$$

For any elements $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_{q^n}$ define

$$e(a) = \omega^{\mathrm{Tr}(a)}, \quad e_n(b) = \omega^{\mathrm{Tr}(\mathrm{Tr}_{q^n \rightarrow q}(b))},$$

where ω is a primitive 3-th root of unity. For a given $a \in \mathbb{F}_q^*$ it is possible to consider the following two Kloosterman sums:

$$K(a) = \sum_{x \in \mathbb{F}_q} e\left(x + \frac{a}{x}\right), \quad K_n(a) = \sum_{x \in \mathbb{F}_{q^n}} e_n\left(x + \frac{a}{x}\right).$$

Denote by $H(a)$ the maximal degree of 3, which divides $K(a)$, and by $H_n(a)$ the maximal degree of 3, which divides $K_n(a)$. Recall that in the case, when $K(a) = 0$ over \mathbb{F}_q , where $q = 3^m$, we assume that 3^m divides $K(a)$, but 3^{m+1} does not divide. There exists a simple connection between $H(a)$ and $H_n(a)$.

Theorem 3.6. *Let $n = 3^h \cdot s$, $n \geq 2$, $s \geq 1$, where 3 and s are mutually prime, and $a \in \mathbb{F}_q^*$. Then*

$$H_n(a) = H(a) + h.$$

The proof follows from two simple statements.

Proposition 3.7. *Let $h = 0$ (that is n and 3 are coprime). Then*

$$H_n(a) = H(a).$$

Proof. By definition of the trace we have for any element $x \in \mathbb{F}_q$

$$\begin{aligned} \mathrm{Tr}(\mathrm{Tr}_{q^n \rightarrow q}(x)) &= \mathrm{Tr}(x + x^q + x^{q^2} + \dots + x^{q^{n-1}}) = \\ &= \mathrm{Tr}(x) + \mathrm{Tr}(x^q) + \mathrm{Tr}(x^{q^2}) + \dots + \mathrm{Tr}(x^{q^{n-1}}) = \\ &= n \mathrm{Tr}(x) = \\ &= \pm \mathrm{Tr}(x), \end{aligned}$$

where the last equality follows, since n and 3 are coprime. Therefore, $\mathrm{Tr}_{q^n \rightarrow p}(x) = 0$ for any $x \in \mathbb{F}_q$, if and only if $\mathrm{Tr}_{q \rightarrow p}(x) = 0$. And, since $a, a^{1/3} \in \mathbb{F}_q$, then all solutions of the equation (2.5) belong to \mathbb{F}_q , that gives the statement. \square

Proposition 3.8. *Let $n = 3$ and $a \in \mathbb{F}_q^*$. Then*

$$H_3(a) = H(a) + 1.$$

Proof. It is known [5] that

$$(3.4) \quad K_3(a) = K(a)^3 - 3K(a)^2 + 3K(a) - 3qK(a).$$

Assume that $K(a)$ is divisible by 3^k . Then it is easy to see that $K_3(a)$ is divisible by 3^{k+1} and is not divisible by 3^{k+2} . \square

From Theorem 3.6, recalling that equality $K(a) = 0$ over \mathbb{F}_q means divisibility of $K(a)$ by q , we immediately obtain the following known result [21].

Corollary 3.9. *Let $a \in \mathbb{F}_q^*$ and $n \geq 2$. Then $K_n(a)$ is not equal to zero.*

REFERENCES

- [1] O. Ahmadi and R. Granger, An efficient deterministic test for Kloosterman sum zeros, *Math. of Computation*, 83 (2014), 347 - 363.
- [2] L.A. Bassalygo and V.A. Zinoviev, On divisibility of exponential sums of polynomials of special type over fields of characteristic 2, in: *Seventh International Workshop on Coding and Cryptography, WCC 2011 (April 11-15, 2011, Paris, France) Proceedings* (eds. D. Augot and A. Canteaut), 2011, 389 - 396.
- [3] L.A. Bassalygo and V.A. Zinoviev, On divisibility of exponential sums of polynomials of special type over fields of characteristic 2, *Designs, Codes and Crypt.*, 66 (2013), 1-3, 129-143.
- [4] L.A. Bassalygo and V.A. Zinoviev, On Kloosterman sums over finite fields of characteristic 3, in: *Proceedings of Thirteenth International Workshop. Algebraic and Combinatorial Coding Theory, ACCT - 13 (June 15-21, 2012), Pomorie, Bulgaria*), 83-87.
- [5] L. CARLITZ, *Kloosterman sums and finite field extensions*, *Acta Arithmetica*, vol. XVI (1969), pp. 179-193.
- [6] P. Charpin, T. Helleseht and V.A. Zinoviev, The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd, *J. Comb. Theory Ser. A*, 114 (2007), 2, 322-338.
- [7] P. Charpin, T. Helleseht and V.A. Zinoviev, On divisibility properties of classical binary Kloosterman sums, *Discrete Math.*, 309 (2009), 12, 3975-3984.
- [8] P. Charpin and G. Gong, Hyperbent functions, Kloosterman sums, and Dickson polynomials, *IEEE Trans. Inform. Theory*, 54 (2008), 9, 4230-4238.
- [9] A. Enge, *Elliptic curves and their applications to cryptography: an introduction*, Klumer Academic Publishers, Boston, 1999.
- [10] F. G'ol'oglu, P. Lisonek, G. McGuire, and R. Moloney, Binary Kloosterman sums modulo 256 and coefficients of the characteristic polynomial, *IEEE Trans. Inform. Theory*, 58 (2012), 4, 2516-2523.
- [11] F. G'ol'oglu, G. McGuire, and R. Moloney, Binary Kloosterman sums using Stickelberger's theorem and the Gross-Koblitz formula, *Acta Arithmetica*, 148 (2011), 3, 269-279.

- [12] F. G'oloğlu, G. McGuire, and R. Moloney, Some results on Kloosterman sums and their minimal polynomials, in: Seventh International Workshop on Coding and Cryptography, WCC 2011 (April 11-15, 2011, Paris, France.), Proceedings (eds. D. Augot and A. Canteaut), 2011, 403 - 412.
- [13] F. G'oloğlu, G. McGuire, and R. Moloney, Some congruences on Kloosterman sums and their characteristic polynomials, J. Number Theory, 143 (2013), 1596-1607; see arXiv:1006.1802v1 [math.NT] 9 Jun 2010.
- [14] G. van der Geer and M. van der Vlugt, Kloosterman sums and the p -torsion of certain Jacobians, Math. Ann., 290 (1991), 3, 549 - 563.
- [15] T. Helleseth and V.A. Zinoviev, On Z_4 -Linear Goethals Codes and Kloosterman Sums, Designs, Codes and Crypt., 17 (1999), 1-3, 246-262.
- [16] T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, IEEE Trans. Inform. Theory, 52 (2006), 2018-2032.
- [17] Katz N. and Livne R., Sommes de Kloosterman et courbes elliptiques universelles en caracteristiques 2 et 3, C. R. Acad. Sci. Paris Ser. I Math., 309 (1989), 11, 723-726.
- [18] Lachaud, G. and Wolfmann, J., The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes, IEEE Trans. Inform. Theory, 36 (1990), 3, 686-692.
- [19] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Reading, MA: Addison Wesley, 20, 1983.
- [20] P. Lisonek, On the connection between Kloosterman sums and elliptic curves, in: Proceedings of the 5th International Conference on Sequences and Their Applications (SETA 2008) (S. Golomb et al. Eds., Lecture Notes in Computer Science, Springer, 5203 (2008), 182 - 187.
- [21] P. Lisonek, and M. Moisisio, On zeros of Kloosterman sums, Designs, Codes and Crypt., 59 (2011), 1 - 3, 223 - 230.
- [22] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, Boston-Dordrecht-London, 1993.
- [23] M. Moisisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, Acta Arithmetica, 132 (2008), 4, 329 - 350.
- [24] M. Moisisio, The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m even, Finite Fields and Their Appl., 15 (2009), 174 - 184.

KHARKEVICH INSTITUTE FOR PROBLEMS OF INFORMATION TRANSMISSION OF THE RUSSIAN ACADEMY OF SCIENCES,, RUSSIA, 127994, MOSCOW, GSP-4, B. KARETNYI PER. 19

E-mail address: bass@iitp.ru, zinov@iitp.ru